

Audit



Report

OFFICE OF THE INSPECTOR GENERAL

**CORRECTIVE ACTIONS ON SYSTEM AND
SOFTWARE SECURITY DEFICIENCIES**

Report No. 95-270

June 30, 1995

20000107 081

Department of Defense

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

ARI 00-04-0891

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit, Audit Planning and Technical Support Directorate, at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Planning and Coordination Branch, Audit Planning and Technical Support Directorate, at (703) 604-8939 (DSN 664-8939) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

Inspector General, Department of Defense
OAIG-AUD (ATTN: APTS Audit Suggestions)
400 Army Navy Drive (Room 801)
Arlington, Virginia 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; (DSN 664-8546) by sending an electronic message to Hotline@DODIG.OSD.MIL; or by writing the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

AFAFC	Air Force Accounting and Finance Center
CA/ACF2	Computer Associates Access Control Facility - 2
CA-NETMAN	Computer Associates Network Manager
DDMS	Defense Debt Management System
DFAS	Defense Finance and Accounting Service
DIPC	Defense Information Processing Center
DISA WESTHEM	Defense Information Systems Agency Western Hemisphere
DISO	Defense Information Services Organization
DJMS	Defense Joint Military Pay System
FSA	Financial Systems Activity
IBM	International Business Machines Corporation
IG	Inspector General
JSS/DOI	Joint Software Service Directorate Operating Instruction
MVS	Multiple Virtual Storage



**INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884**



June 30, 1995

**MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (COMPTROLLER)
ASSISTANT SECRETARY OF DEFENSE (COMMAND,
CONTROL, COMMUNICATIONS AND
INTELLIGENCE)
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING
SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS
AGENCY**

**SUBJECT: Audit of Corrective Actions on System and Software Security Deficiencies
(Report No. 95-270)**

We are providing this final report for management's information and use. We performed this audit at the request of the Under Secretary of Defense (Comptroller) and the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) to follow up on previously identified deficiencies in software security. Management comments on a draft of this report were considered in preparing the final report.

The comments on the draft of this report conformed to the requirements of DoD Directive 7650.3, and there are no unresolved issues. Therefore, no additional comments are required.

The courtesies extended to the audit staff are appreciated. Questions on this audit should be directed to Mr. Christian Hendricks, Program Director, at (703) 604-9139 (DSN 664-9139) or Mr. Kent E. Shaw, Project Manager, at (703) 604-9152 (DSN 664-9152). Appendix C lists the distribution of this report. The audit team members are listed inside the back cover.

**Robert J. Lieberman
Assistant Inspector General
for Auditing**

Office of the Inspector General, Department of Defense

Report No. 95-270
(Project No. 4FG-5060)

June 30, 1995

**Corrective Actions on System and
Software Security Deficiencies**

Executive Summary

Introduction. The audit was made at the request of the Under Secretary of Defense (Comptroller) and the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) to confirm that the Defense Finance and Accounting Service had implemented corrective actions on software development deficiencies identified in two prior audit reports issued by the Inspector General, DoD:

- o Report No. 94-060, "General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization," March 18, 1994, and

- o Report No. 94-065, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," March 24, 1994.

Those two reports addressed general controls and selected features of the operating systems and security software used by the Defense Information Systems Agency Western Hemisphere (formerly the Defense Information Services Organization) and the Defense Finance and Accounting Service to control access to critical information systems. Those information systems manage information used in the preparation of annual financial statements for DoD and perform various other financial management and payment functions.

Objectives. The overall objective of this audit was to determine whether the Defense Finance Accounting Service had corrected system and personnel security deficiencies at its central design activities identified in the two prior Inspector General, DoD, audit reports.

Audit Results. After the prior audits, the Financial Systems Activities at Pensacola, Florida, and Denver, Colorado, improved controls over access to critical computer systems, software changes, and quality assurance procedures; however, seven of the eight recommendations to the Defense Finance and Accounting Service in Reports No. 94-065 and No. 94-060 were not yet fully implemented.

- o **Access Control.** Financial Systems Activity Pensacola had not complied with Defense Information Systems Agency guidelines on password length, and had not set up its computer security software to properly control started tasks. Additionally, although the Financial Systems Activity Pensacola had established off-site storage of critical tape files for system backup, these tape files were stored in a facility that was at risk of compromise because keys to the facility were not properly controlled. As a result of those access control problems, the Multiple Virtual Storage Operating System and the payroll application program at the Financial Systems Activity Pensacola continued to be exposed to an increased risk of unauthorized access. However, the Financial Systems Activity Pensacola was taking corrective actions on the deficiencies (Finding A).

o Change Management Procedures. The Financial Systems Activity Pensacola had not fully established change management procedures to control and track changes to the Multiple Virtual Storage operating system. The Financial Systems Activity Denver had not established procedures to manage software changes for all central design activity divisions at the Financial Systems Activity Denver; had not fully segregated the responsibilities for making program changes, performing system tests, and moving changed programs into production for the Defense Debt Management System Division; and had not enforced coordination requirements for existing procedures to manage software changes. As a result, the integrity of the operating system at the Financial Systems Activity Pensacola was threatened, and key financial applications at the Financial Systems Activity Denver were exposed to an increased risk of unauthorized program changes (Finding B).

Potential Benefits of Audit. We did not identify any potential monetary benefits in this audit. However, if recommendations in this report are implemented, controls over unauthorized access and changes to critical software will be improved. See Appendix A for details of those benefits.

Summary of Recommendations. We recommended that the Defense Finance and Accounting Service strengthen controls over access and change management for critical computer systems. The Assistant Inspector General for Analysis and Followup closed Recommendations A.3., B.3., and C.2.a. of Report No. 94-065 and Recommendation E.2. of Report No. 94-060 based on information from the Defense Finance and Accounting Service. However, during our fieldwork, we determined that those recommendations had not been fully implemented. As a result, those recommendations have been reopened. We recommended that separate comments be provided for those recommendations.

Management Comments. Comments were received from the Under Secretary of Defense (Comptroller), the Defense Finance and Accounting Service, and the Defense Information Systems Agency. The full text of those comments is in Part IV. The Under Secretary of Defense (Comptroller), to whom no recommendations were directed, had no objections to the report. The Defense Finance and Accounting Service and the Defense Information Systems Agency concurred with all the findings and recommendations.

Audit Response. Comments from the Defense Finance and Accounting Service and the Defense Information Systems Agency were responsive. Although separate comments were not provided for the original recommendations, as requested in our draft report, those recommendations have been implemented, as have the recommendations in this report. Corrective actions had been taken on all recommendations made to the Financial Systems Activity Denver. Also, on March 31, 1995, the Defense Information Systems Agency assumed all responsibility for operating system maintenance at the Financial Systems Activity Pensacola. For these reasons, no followup action will be required for recommendations in this report, and all recommendations addressed in this report were closed. We look forward to working closely with management in the future to identify further challenges and opportunities for improvement in the information systems security area.

Table of Contents

Executive Summary	i
Part I - Introduction	1
Background	2
Weaknesses Identified in Previous Reports	3
Objectives	4
Scope and Methodology	5
Management Controls	5
Prior Audits and Other Reviews	6
Part II - Findings and Recommendations	9
Finding A. Access Control	10
Finding B. Software Change Management	18
Part III - Additional Information	29
Appendix A. Summary of Potential Benefits Resulting From Audit	30
Appendix B. Organizations Visited or Contacted	31
Appendix C. Report Distribution	32
Part IV - Management Comments	
Under Secretary of Defense (Comptroller) Comments	36
Defense Finance and Accounting Service Comments	37
Defense Information Systems Agency Comments	41

This report was prepared by the Finance and Accounting Directorate, Office of the Assistant Inspector General for Auditing, Department of Defense.

Part I - Introduction

Introduction

Background

From 1992 through 1994, the Inspector General (IG), DoD, issued four audit reports on controls over Defense automated operating systems. Those reports included:

- o Report No. 94-065, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," March 24, 1994;

- o Report No. 94-060, "General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization," March 18, 1994;

- o Report No. 93-133, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," June 30, 1993; and

- o Report No. 93-002, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," October 2, 1992.

The reports outlined specific weaknesses and management control problems at activities of the Defense Information Systems Agency (DISA), the Defense Finance and Accounting Service (DFAS), the Defense Logistics Agency, and the Marine Corps Computer and Telecommunications Activity. Recommendations in those reports addressed weaknesses in operating system configuration, access control, and continuity of operations at DISA and DFAS activities. Additionally, recommendations were aimed at improving management practices and addressing weak management controls over computer systems at those activities.

The DFAS operates central design activities, called Financial Systems Activities (FSAs), at Denver, Colorado (FSA Denver); Indianapolis, Indiana (FSA Indianapolis); Pensacola, Florida (FSA Pensacola); Columbus, Ohio (FSA Columbus); Cleveland, Ohio (FSA Cleveland); and Kansas City, Missouri (FSA Kansas City). The FSAs are responsible for developing and maintaining DFAS financial systems. The Financial Systems Organization, Indianapolis, Indiana, oversees the management of the FSAs. The Defense Information Systems Agency Western Hemisphere (DISA WESTHEM) owns and operates the computers and related operating systems that the FSAs use. Both DISA WESTHEM and DFAS are part of the Defense Business Operations Fund, a revolving fund, which provides goods and services to other Defense activities on a cost-reimbursable basis.

This audit focused on deficiencies that the reports identified at FSA Pensacola and FSA Denver, and at the Defense Information Processing Center in Pensacola, Florida, formerly the Naval Computer and Telecommunications

Station. The FSAs are DFAS-owned central design activities that are responsible for programming and maintenance for DFAS financial software such as the Defense Debt Management System and the Defense Joint Military Pay System, Active and Reserve Component. The FSAs report to the DFAS Financial Systems Organization in Indianapolis. The Defense Information Processing Center, Pensacola, Florida, provides computing services for the FSA Pensacola and other Defense activities.

On July 12, 1994, the Under Secretary of Defense (Comptroller)* and the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) requested that the Inspector General (IG), DoD, meet with DFAS and DISA to confirm that corrective actions had been completed on security weaknesses identified by the four reports. Two audits were initiated in response to this request. The audit of corrective actions taken at DFAS was assigned Project No. 4FG-5060, "Audit of Corrective Actions on Application Software Deficiencies." The followup audit for DISA and the Defense Logistics Agency was assigned Project No. 4FD-5068, "Followup Audit of Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service."

This report discusses the corrective actions taken on recommendations at the DFAS activities in response to Reports No. 94-065 and No. 94-060. A report on the corrective actions taken by DISA and the Defense Logistics Agency will be issued separately.

Weaknesses Identified in Previous Reports

In IG, DoD, Report No. 94-065, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," March 24, 1994, we determined that operating system controls at FSA Pensacola needed improvement.

Specifically, access to sensitive system libraries and programs was not adequately monitored and controlled; programmers had installed vendor supervisor calls (powerful system management routines) that compromised system integrity; critical backups to system software were not being stored off-site; and sensitive system programmer positions were not designated as critical-sensitive. As a result, we recommended that the Director, Defense Finance and Accounting Service Financial Systems Activity, Pensacola, Florida:

o fully implement the installation integrity guidelines being developed by DISA to emphasize the integrity and security of time share options, authorized program facility commands, vendor supervisor calls, and sensitive utilities;

*Formerly the Comptroller of the Department of Defense.

Introduction

- o identify all started tasks to the mainframe security software and define individual security accesses to each;
- o implement formal change management procedures for changes to the computer operating system;
- o designate all system programmer positions as critical-sensitive and perform appropriate background investigations; and
- o store backups of critical operating system files in an off-site location.

In IG, DoD, Report No. 94-060, "General Controls for Computer Systems at the Defense Information Processing Centers of the Defense Information Services Organization," March 18, 1994, we found that application program changes at FSA Denver were not always properly authorized and approved, and that separation of duties was sometimes compromised when moving completed program changes into production. The following recommendations were addressed to the Director, Defense Finance and Accounting Service Financial Systems Activity, Denver, Colorado:

- o require that all DFAS central design activities follow procedures similar to those established in Joint Service Software Directorate Operating Instruction 205-3, "Computer Security, Program Module Certification," December 1, 1991;
- o segregate the responsibilities for making program changes, performing tests, and moving changed systems into production; and
- o enforce the coordination requirements in Joint Service Software Directorate Operating Instruction 205-3 for making program changes to the Joint Service System for active components and the Joint Service System for Reserve Components.

Part II of this report, "Findings and Recommendations," describes weaknesses found 6 months after the issuance of the final audit reports identifying those weaknesses. Additionally, Part II addresses one weakness that was not identified during the original audit.

Objectives

The overall objective of the audit was to determine whether the FSAs had corrected the system and personnel security deficiencies identified in two prior IG, DoD, audit reports.

Scope and Methodology

Time Period, Standards, and Locations. We performed this audit from July through October 1994. We visited or contacted FSA Denver, FSA Indianapolis, and FSA Pensacola. In addition, we visited the Naval Computer and Telecommunications Station (now the Defense Information Processing Center), Pensacola, Florida, and Headquarters, DFAS, Arlington, Virginia. We contacted the Federal Emergency Management Agency in Baltimore, Maryland, and Atlanta, Georgia, and the National Institute of Standards and Technology, Gaithersburg, Maryland, to obtain standards on adequately protecting off-site storage space from disaster. A complete list of organizations visited or contacted is in Appendix B. The audit was made in accordance with auditing standards issued by the Comptroller General of the United States as implemented by the IG, DoD.

Scope of Our Review. At the FSAs in Denver, Indianapolis, and Pensacola, we interviewed key personnel and obtained pertinent information. We evaluated those data to determine whether management had implemented the recommendations. We also reviewed security policies and access to the systems, programs, and data. Because the audit was limited to an analysis of management actions taken in response to recommendations in the prior IG, DoD, reports, we did not review all general or application controls pertaining to the FSAs or the automated systems. We did not use statistical sampling procedures to conduct this audit.

Computer-Processed Data. We relied on standard International Business Machines Corporation (IBM) utility programs and standard reports provided by commercial security software packages to satisfy our audit objective. We also used a commercial software package marketed by Computer Associates International, Incorporated (CA), CA/EXAMINE, to analyze the IBM operating system at FSA Pensacola. Data from two security software packages, CA/TOP SECRET and Computer Associates Access Control Facility Version 2 (CA/ACF2), were used to assess security rules and features. Specifically, we obtained lists of control parameters that authorize computer programs and personnel to access data. To test reports generated by the commercial software packages, we used the same terminals that were normally used to gain access to system resources. All system testing and use of audit software was done in a controlled environment with management's approval. Based on those tests, we concluded that the data were sufficiently reliable to meet the audit objective and support our audit conclusions.

Management Controls

Controls Assessed. We reviewed corrective actions taken at FSA Pensacola, FSA Denver, and FSA Indianapolis. Our review included assessments of background investigation practices, access controls, and controls over changes

Introduction

to system and application programs. Our audit showed that DFAS had performed the reviews of management controls required by DoD 5010.38, "Internal Management Control Program," April 14, 1987.

DFAS Statement of Assurance. The DFAS Annual Statement of Assurance for FY 1994 reported 51 uncorrected material management control weaknesses in the Defense Finance and Accounting Service system of internal accounting and administrative controls. The following weaknesses identified in the Annual Statement of Assurance were relevant to our review:

- o FSA Denver's application security weaknesses were a lack of segregation of duties between programmers and certifiers in the Defense Debt Management System (DDMS) and excessive access to production libraries of the Defense Joint Military Pay System (DJMS) Active Component and the DJMS Reserve Components. Those deficiencies were also identified during our audit, and are discussed in Findings A and B of this report.

- o Operating system and security software weaknesses applicable to change management procedures and access controls existed at FSA Pensacola. Those deficiencies were also identified during our audit and are discussed in Findings A and B of this report.

- o Computer security weaknesses existed at FSA Indianapolis; those weaknesses included a lack of controls over operating system software and distribution of source code, and a lack of contingency resources. Although our audit did not focus on security problems at FSA Indianapolis, we identified problems with computer security at other FSAs. See Finding A for a discussion of the problems we identified.

Management Control Weaknesses Identified. Although we found management control weaknesses pertaining to access controls and change management controls, management has made significant improvements in the areas identified in the previous reports and in the DFAS Annual Statement of Assurance for 1994. As a result of these improvements, we no longer consider those weaknesses to be material, although additional corrective action is required.

Benefits of Audit. No monetary benefits will result from correcting the management control weaknesses. However, implementation of our recommendations will improve the overall security and management control of the audited systems. Other benefits are explained in Appendix A, "Summary of Potential Benefits Resulting From Audit."

Prior Audits and Other Reviews

We identified four IG, DoD, audit reports and two Air Force Audit Agency reports that were relevant to our review.

IG, DoD. The following IG, DoD reports identified a number of system and software security deficiencies.

- o Report No. 94-065, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," March 24, 1994, identified problems with management controls over selected features of the operating system and security software used by elements of the DISO, the DFAS, and the Marine Corps.

- o Report No. 94-060, "General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization," March 18, 1994, addressed general controls at DISO information processing centers that support the FSA Denver.

- o Report No. 93-133, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," June 30, 1993, addressed serious deficiencies in the implementation and control of operating system and security software at the Defense Logistics Agency Automation Center and the Defense Information Technology Service Organizations at Dayton and Columbus, Ohio.

- o Report No. 93-002, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," October 2, 1992, showed that the Defense Information Technology Service Organizations at Dayton and Columbus, Ohio, had serious deficiencies in implementing and controlling operating system and security software.

Part II of this report lists the recommendations made in the two prior reports for which we performed followup work (Reports No. 94-060 and No. 94-065), summarizes management's comments on those recommendations, and gives the results of our followup evaluation of actions taken on those recommendations.

Air Force Audit Agency. Two Air Force Agency reports covered security software and backup and disaster recovery plans.

- o Report No. 1265611, "Review of the Contingency Plan for Continued Operations of DFAS-DE Centralized Pay and Accounting Systems," September 5, 1991, identified weaknesses in backup and disaster recovery controls at FSA Denver. That report concluded that contingency planning for audited systems needed improvement in production of backup tapes and site testing.

- o Report No. 0195410, "Data Processing Center Operations and Security at the Air Force Accounting and Finance Center (AFAFC)," August 5, 1991, identified weaknesses in the operating system and security software features and controls over data security and integrity at the AFAFC (now Defense Megacenters Denver).

This page was left out of original document

Part II - Findings and Recommendations

Finding A. Access Control

Although significant improvements had been made since the two IG, DoD, reports were issued in March 1994, controls over access to critical financial computer resources needed to be strengthened. Specifically:

- o FSA Pensacola had not complied with DISA guidelines concerning password length, found in "DISA WESTHEM Personnel and Security: MVS Security Technical Implementation Standards," December 29, 1994;

- o FSA Pensacola had not complied with the DISA guidelines, listed above, for control of started tasks by the security software; and

- o the Defense Information Processing Center, Pensacola, Florida (DIPC Pensacola), had not provided proper control over keys to the storage facility for backup tapes.

FSA Pensacola had not complied with DISA guidelines on password length because they believed the guidelines were inappropriate for their system. Started tasks were not properly controlled by the security software because the started tasks were assigned a default logon identification. Keys to the storage facility for backup tapes at the DIPC Pensacola were not properly controlled because procedures for their control were not in place or were not being enforced. As a result of those deficiencies, the Multiple Virtual Storage Operating System and the payroll application program at FSA Pensacola continued to be exposed to an increased risk of unauthorized access. However, FSA Pensacola was taking corrective action on the deficiencies.

Background

Access Control Software. Computer facility managers often use commercial security software packages to provide additional protection and controls. Those commercial security software packages work in conjunction with other controls to protect the system from unauthorized access. FSA Pensacola used CA/ACF2 for that purpose. FSA Denver used CA-TOP SECRET security software.

Other Controls. In addition to automated access controls provided by the security software packages, management relies on other administrative controls to ensure that computer resources are properly protected. Those controls should include separation of duties, personnel security, and physical security over the computer and its backup facilities.

Office of Management and Budget Circular No. A-130, "Management of Federal Information Sources," December 24, 1985, requires Federal agencies to ensure that data files, computer programs, and equipment are protected from unauthorized changes, unauthorized disclosure and use, and destruction.

DISA Installation Integrity Guidelines

IG, DoD Report No. 94-065, Recommendation A.3., "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service." *We recommend that the Director, Defense Finance and Accounting Service, Financial Systems Activity, Pensacola, Florida, fully implement the IBM-recommended installation integrity guidelines currently being developed by the Director, Defense Information Services Organization. In implementing those guidelines, particular emphasis should be placed on evaluating the integrity and security of time share options, authorized program facility commands, vendor supervisor calls, and sensitive utilities.*

Management Response. In its response, dated January 24, 1994, FSA Pensacola concurred and stated that all control deficiencies in operating systems under the cognizance of FSA Pensacola, as noted in the draft audit report, had been corrected during the audit. FSA Pensacola management stated that the remaining recommendation for implementation of DISO guidelines, which were being developed, would be pursued when the guidelines were promulgated.

Audit Followup. The Assistant Inspector General for Analysis and Followup had closed Recommendation A.3. of Report No. 94-065 based on the DFAS response to the report. However, as a result of our fieldwork, that recommendation has been reopened pending adequate action.

Results of Followup on Recommendation A.3. FSA Pensacola management had completed action to correct prior weaknesses in authorized program facility libraries, non-IBM supervisor calls, controls over sensitive utilities, and tape security bypass controls.

FSA Pensacola had not fully implemented proper controls over started tasks. Because Recommendation B.3. of the same report said that started tasks should be identified to the security system, started tasks are discussed in greater detail under that recommendation. Additionally, FSA Pensacola had not fully implemented the requirement for password length in the guidelines.

Integrity Guidelines. IBM publishes integrity guidelines for systems that run its Multiple Virtual Storage operating system. IBM document GC28-1400-0,

Finding A. Access Control

"IBM Multiple Virtual System Security Guidelines," March 1984, specifies system parameters, settings, principles, and practices for system managers to implement and follow to enhance the security of their systems and to prevent unauthorized access, modification, or destruction of system resources. On August 9, 1994, DISA issued a policy memorandum, "International Business Machines (IBM) Multiple Virtual Storage (MVS) Security Policy," which recommended that specific security guidelines be implemented on DISA-managed DoD financial systems using the MVS operating system. Although the DISA memorandum did not apply to the FSA Pensacola system, FSA Pensacola management agreed in their response to IG, DoD, Report No. 94-065 that the DISA standard, then in development, would be used as a guide to implement our audit recommendations.

Password Length

FSA Pensacola had not fully implemented the requirement in the Defense Information Systems Agency (DISA) integrity guidelines for an eight-character password, but instead used a five-character password. After reviewing the DISA integrity guidelines, FSA Pensacola determined that the eight-character password would not be cost-effective to implement. In an October 25, 1994, letter to DISA, FSA Pensacola requested a waiver of the password requirements. It stated that implementing the requirements was unnecessary and costly. Although FSA Pensacola management could not provide estimates of costs or additional manpower requirements to support their contention that implementation would be too costly, DISA agreed to review the request for waiver.¹

Other Criteria on Password Length. The DoD Computer Security Center Standard 002-85, "Department of Defense Password Guideline," April 12, 1985, provides guidance for implementation of passwords on DoD systems. Those criteria state that passwords should be at least six characters.

Started Tasks

IG, DoD, Report No. 94-065, Recommendation B.3., "Controls Over Operating System and Security Software Supporting the Defense Finance

¹As a result of that review, DISA rewrote the guidelines to require a six-character password instead of the eight-character password.

and Accounting Service." *We recommend that the Director, Defense Finance and Accounting Service, Financial Systems Activity, Pensacola, Florida, direct the Information System Security Officer to identify, on both systems, all started tasks to the Computer Associates International, Inc., Access Control Facility Version 2 security software, and grant appropriate access to each started task.*

Management Response. In its response, dated January 24, 1994, FSA Pensacola concurred and stated that corrective action was complete. FSA Pensacola management stated that the following controls over started tasks had been implemented on both systems to correct the stated deficiency:

- o The CA/ACF2 global started task control feature was turned on (the CA/ACF2 default is OFF) and appropriate started task logon identifications were established to implement validation of dataset access for all started tasks.

- o Access to controlled libraries was closely monitored, and the number of personnel with the ability to make changes to the controlled libraries was limited to the eight employees assigned to the FSA Pensacola systems division.

Audit Followup. The Assistant Inspector General for Analysis and Followup closed Recommendation B.3. of Report No. 94-065 based on the DFAS response to the report. However, as a result of our fieldwork, that recommendation has been reopened pending adequate action.

Results of Followup on Recommendation B.3. FSA Pensacola had not uniquely identified all started tasks to the CA/ACF2 security system.

Started tasks are programs that are automatically executed during system startup and continue to run during system operations. Unless uniquely defined, started tasks can more readily bypass security software controls. To prevent started tasks from accessing unauthorized files or programs, started tasks need to be uniquely identified to the computer's security software. If a started task tries to access unauthorized computer programs or data files, the task is terminated or canceled.

Access Controls Over Started Tasks. FSA Pensacola had access controls in place for the started tasks, but a more secure approach was available. FSA Pensacola used a started task "default" identifier. The default identifier allowed the started tasks to execute even if they had not been individually identified to the security software. To compensate, FSA Pensacola limited the access ability of the started tasks at the file and program level.

Finding A. Access Control

A better approach is to uniquely identify each started task to the security software and avoid using default identifiers. When that method is used, the controls over started tasks take effect earlier in the execution process and do not permit unidentified started tasks to execute at any level.

Non-Cancel Status. FSA Pensacola personnel were implementing the non-default option. Specifically, all started tasks had been assigned unique logon identifications. However, until tests were done to ensure the integrity of the new configuration, they had assigned "non-cancel" to the individual started task jobs. The non-cancel designation meant that any of the started tasks that violated security rules would continue operating, rather than being automatically terminated by the security software. System managers assigned non-cancel status to the started tasks so that critical system jobs would not terminate in the event of operator error. Although that was a prudent method of implementing unique identification codes, the non-cancel status assigned to the started task still presented a security weakness. Started tasks with a non-cancel status could be used to circumvent security software.

System managers stated that the non-cancel status was necessary during implementation of the new configuration. The intention was to remove the non-cancel designation from the started job tasks after the system manager had completed tests and adjustments of the new configuration. That action had not taken place; therefore, until the non-cancel designation has been removed, action has not been completed on the original recommendation. When testing of the new configuration is complete, the system manager should remove the non-cancel status from the started tasks.

Background Investigation of System Programmers

IG, DoD, Report No. 94-065, Recommendation C.2.b., "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service." *We recommend that the Director, Defense Finance and Accounting Service, Financial Systems Activity, Pensacola, Florida, require that all system programmer positions be designated critical-sensitive and that appropriate background investigations be obtained for personnel assigned to those positions.*

Management Comments. In its response, dated January 24, 1994, FSA Pensacola concurred and stated that sensitive positions had been identified and actions initiated to change the position descriptions to designate those positions as critical-sensitive. FSA Pensacola estimated that position description changes and background investigations would be completed in 180 days.

Results of Followup on Recommendation C.2.b. All system programmers at FSA Pensacola had been designated as critical-sensitive, and appropriate background investigations had been initiated by Headquarters, DFAS. Actions taken on this recommendation are fully responsive.

Security Over Tape Backup

IG, DoD, Recommendation, Report No. 94-065, Recommendation C.2.c., "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service." *We recommend that the Director, Defense Finance and Accounting Service, Financial Systems Activity, Pensacola, Florida, request that the Naval Computer and Telecommunications Station [NCTS], Pensacola, Florida, store backups of critical Multiple Virtual Storage operating system files at an off-site location.*

Management Response. In its response, dated January 24, 1994, FSA Pensacola concurred and stated that an automated cartridge system had been installed and all backup tape operations had been switched from 9-track reels to automated cartridges. FSA Pensacola stated that procedures were being developed for identifying and ejecting the appropriate cartridges for routing to off-site storage, and changes were being made to the level-of-service agreement between FSA Pensacola and NCTS Pensacola to implement off-site storage. The estimated completion time for required actions was 180 days.

Results of Followup on Recommendation C.2.c. Management had begun storing backup tapes of critical system files in a building adjacent to the processing center. We initially had concerns about the close proximity of the storage facility to the processing center and about its location on the Gulf of Mexico, where flooding and hurricanes are a risk. We determined from the Federal Emergency Management Agency that the storage facility is located in a 500-year floodplain. That means that a 0.02-percent chance of flooding exists each year. We regard that as an acceptable risk. We also learned that the file tapes, if destroyed, could be replaced by alternate DFAS sites or the operating system vendor. Therefore, we consider corrective action on this recommendation complete.

Keys to Storage Facility

Although the selected storage site was adequate, the keys to the storage facility were not kept in a secure storage locker or under the control of a responsible

Finding A. Access Control

custodian. As a result, any employee with access to the processing center could enter the tape storage facility and alter or destroy the tapes. To ensure the integrity of the tape backup facility, installation managers should maintain proper control over keys.

Summary

As shown by Table 1, DFAS management has either completed or is implementing corrective action on all four prior recommendations pertaining to access controls. Management's comments on this report should update the status of actions taken to satisfy recommendations listed as "in progress."

**Table 1. Status of Original Recommendations
Pertaining to Access Controls**

<u>Report Number</u>	<u>Recommendation</u>	<u>Management Action</u>
94-065	A.3.	In progress
	B.3.	In progress
	C.2.b.	Complete
	C.2.c.	Complete*

*Better controls over keys to the tape backup storage facility were needed.

Recommendations, Management Comments, and Audit Response

1. We recommend that the Director, Defense Finance and Accounting Service Financial Services Activity, Pensacola, Florida:

a. Implement the use of passwords that have at least six characters.

Management Comments. The Deputy Director for Information Management, DFAS, concurred. Effective February 12, 1995, the password length requirement for the two platforms supported by FSA Pensacola was modified to reflect a minimum of six characters. DFAS considers this recommendation closed.

Finding A. Access Control

Audit Response. The action taken by the DFAS is fully responsive to the recommendation.

b. Complete testing and remove the "non-cancel" parameters from the started task jobs.

Management Comments. The Deputy Director for Information Management, DFAS, concurred. Effective January 1995, non-cancel was removed from all started tasks on the platforms supported by FSA Pensacola.

Audit Response. The action taken by the DFAS is fully responsive to the recommendation.

2. We recommend that the Director, Defense Information Processing Center, Pensacola, Florida, develop and implement procedures to provide safeguards over keys to the off-site storage facility for backup tapes.

Management Comments. The Inspector General, DISA, concurred with the finding and recommendation. The Inspector General stated that the DIPC Pensacola has secured the keys to the tape backup facility. The keys are locked in a key container in the equipment room of DIPC Pensacola. The DIPC Pensacola equipment room is a controlled area accessible only to individuals who work in the area and have had appropriate background investigations. The key to the storage facility is controlled by the senior official on each shift.

Audit Response. The action taken by the DISA is fully responsive to the recommendation.

Finding B. Software Change Management

Although some improvements had been made since the two IG, DoD reports were issued in March 1994, procedures for software change management (management controls over software changes) at both FSA Pensacola and FSA Denver continued to need improvement. FSA Pensacola management had not implemented change control procedures for reviewing and approving changes to the operating system. Management had planned to use a commercial software package to support that effort; however, FSA Pensacola personnel lacked expertise with the software, and management had not established interim procedures. FSA Denver had not established procedures to manage software changes for all of its central design activity divisions; managers relied on each division to establish change management procedures and segregate duties. Consequently, these procedures were poorly coordinated and often were not formalized. FSA Denver had not fully segregated responsibilities for making program changes, performing system tests, and moving changed programs into production for the Defense Debt Management System Division; a separate production group had not been established, and change management procedures had not been implemented. Finally, because of poor coordination, formalized change control procedures often were not effectively enforced. As a result, the integrity of the operating systems was threatened and key financial applications were exposed to an increased risk of unauthorized program changes.

Background

Change management procedures are management controls designed to ensure that authorized software changes to a system have been properly approved, documented, and implemented. Those procedures usually include a method for recording and tracking such changes. Change management procedures usually consist of a governing instruction specifying the forms to be used and procedures to be followed, including procedures for supervisory review and approval prior to implementing the changes. Change management procedures must be combined with appropriate access controls to ensure that system security features are not circumvented.

The FSA Denver central design activity has 16 divisions, each with responsibility for the management of a computer system. IG, DoD, Report No. 94-060 reviewed the divisions of the central design activity that has responsibility for the Defense Debt Management System (DDMS), the Defense Joint Military Pay System (DJMS) Active Component and the DJMS Reserve Component. Additionally, management responses to IG, DoD, Report No. 94-060 referenced only those divisions. Because original audit coverage

and management's response referenced only those three divisions, we limited our review at FSA Denver to those divisions of the central design activity with responsibility for the DDMS, the DJMS Active Component, and the DJMS Reserve Component.

Change Management Procedures for FSA Pensacola Operating System

IG, DoD, Report No. 94-065, Recommendation C.2.a., "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service." *We recommend that the Director, Defense Finance and Accounting Service, Financial Systems Activity, Pensacola, Florida, require the Director, Technology Support Activity, to establish formal change management procedures to control the processing of all changes to the Multiple Virtual Storage operating system.*

Management Response. In its response, dated January 24, 1994, FSA Pensacola concurred and stated that its goal is to incorporate the formal standards for executive software configuration management that were being developed in conjunction with site consolidation and standardization. However, since selection and incorporation of standard products and procedures for executive software configuration management was still a future event, interim procedures were being developed locally for configuration management of the executive software suites for the FSA Pensacola production systems. FSA Pensacola was implementing fully functional configuration management processes, mechanized through CA-NETMAN (Computer Associates Network Manager [CA-NETMAN]) software. FSA Pensacola had procured and installed CA-NETMAN software and had identified all currently installed executive software products as components of the CA-NETMAN data base to establish a baseline for inventory tracking and change management. Additional customization and the development of procedures were required to achieve a fully functional, user-friendly environment for change management. The customization and development of local procedures was expected to be complete in approximately 180 days.

In its response to an inquiry from the Assistant Inspector General for Analysis and Followup, DFAS Headquarters stated on October 4, 1994, that FSA Pensacola had developed standards for configuration management and issued those standards to the Defense megacenters; installed CA/Netman to establish a baseline for inventory tracking and change management; and issued taskings to customize the product to achieve fully functional MVS change management. According to DFAS Headquarters, these changes were started in October 1993 and completed in August 1994.

Finding B. Software Change Management

Audit Followup. The Assistant Inspector General for Analysis and Followup closed Recommendation C.2.a. of Report No. 94-065 based on information forwarded to them by the DFAS in October 1994, as summarized above. However, as a result of our fieldwork, that recommendation has been reopened pending adequate action.

Results of Followup on Recommendation C.2.a. Local procedures to control and track MVS operating system changes had not been developed. FSA Pensacola provided us with a draft copy of an "Executive Software Configuration Management Plan," but because the draft had not been finalized and the plan relied on Computer Associates Network Manager (CA-NETMAN) software that had not been fully implemented at FSA Pensacola, we did not consider managements action to be fully responsive. FSA Pensacola officials told us that they lacked the expertise in CA-NETMAN that they believed was necessary to develop such procedures. Consequently, FSA Pensacola management contracted for full implementation of the CA-NETMAN program during summer 1994.

Change Management Procedures at FSA Denver

IG, DoD, Report No. 94-060, Recommendation E.1., "General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization." *We recommend that the Director, Defense Finance and Accounting Service, Financial Systems Activity, Denver, Colorado, require that, at a minimum, all central design activities follow procedures similar to those established in Joint Service Software Directorate Operating Instruction 205-3.*

Management Response. In response to the draft audit report, FSA Denver concurred and stated that it would perform a review to ensure that procedures identical or similar to those established in Joint Service Software Directorate Operating Instruction 205-3 (JSS/DOI 205-3) were followed. Strong emphasis had been placed on the importance of proper certification for movement of program modules. The review would be accomplished as part of the FY 1994 management control review, to be completed by September 30, 1994.

Results of Followup on Recommendation E.1. FSA Denver stated that it would perform a review to ensure that all central design activities were following procedures identical or similar to those established in JSS/DOI 205-3. However, JSS/DOI 205-3 was superseded by DFAS DE/FJ Instruction 5200.1 (DFAS DE/FJ 52001.1), "Computer Security, Program Module Certifications," November 23, 1993. This instruction established policy, responsibilities, and procedures for adequate software change control, movement of modules to system testing and production, and specification of contents for a certification package. We reviewed implementation of the recommendation at 3 of the 16 central design activity divisions operated by FSA Denver. Those three divisions had responsibility for the DDMS, the DJMS Active Component, and the DJMS Reserve Component.

Finding B. Software Change Management

The central design activity for the DDMS had not adopted procedures for the control of change management as recommended in IG, DoD, Report No. 94-060. The central design activity for the DJMS Active Component had not effectively implemented procedures. Only the central design activity for the DJMS Reserve Component had effectively implemented appropriate change management criteria.

IG, DoD, Report No. 94-060, Recommendation E.1., recommended that the FSA Denver adopt criteria similar to JSS/DOI 205-3, December 1, 1991. After fieldwork was completed for IG, DoD, Report No. 94-060, however, JSS/DOI 205-3 was replaced by DFAS-DE/FJ Instruction 5200.1, "Software Change Control," November 29, 1993. That instruction provides stricter procedures for controlling software changes.

DFAS-DE/FJ 5200.1 provides a standard certification review sheet and states that newly developed, modified, or revised program modules shall not be moved into the production environment until the certification process has been completed. Appendix 4 of DFAS-DE/FJ Instruction 5200.1 presents detailed instructions for the completion of certification move sheets. The appendix specifies:

The following signatures in the signature blocks identified are mandatory and must be different signatures for Programmer, Certifier, System Analyst, System Test Branch Chief, System or Functional Tester, Customer approval, and Production Move Monitor. This is to assure accountability for checks and balances . . .

Defense Debt Management System. We found that the DDMS had not implemented operating procedures similar to JSS/DOI 205-3 as recommended in IG, DoD, Report No. 94-060. Using DFAS-DE/FJ Instruction 5200.1, we reviewed all of the 81 certification move sheets completed by the DDMS Directorate from May through September 1994. We determined that application program changes at FSA Denver were not properly authorized and approved when moving program changes into production. Table 2 provides a detailed analysis of problems.

Finding B. Software Change Management

Table 2. DDMS Noncompliance Wwith DFAS-DE/FJ Instruction 5200.1.

<u>Type of Noncompliance</u>	<u>Number of Instances</u>	<u>Percentage of Total</u>
Programmer signed as certifier	54	66.7
Certifier did not sign	26	32.1
Neither certifier nor programmer signed	<u>1</u>	<u>1.2</u>
Total	81	100.0

Subsequent to our audit fieldwork, FSA Denver management finalized procedures requiring DDMS to follow DFAS-DE/FJ Instruction 5200.1. That instruction is similar to JSS/DOI 205-3, referred to in Recommendation E.1. of IG, DoD, Report No. 94-060. We will consider management action for DDMS responsive to this recommendation when the new procedures have been properly implemented.

Defense Joint Military Pay System. Our review of the central design activities of DJMS showed that the DJMS Reserve Component had effectively implemented criteria for change management. The DJMS Active Component was supposed to follow the same procedures as the DJMS Reserve Component, but had not effectively implemented the procedures.

Separation of Duties

IG, DoD, Report No. 94-060, Recommendation E.2., "General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization." *We recommend that the Director, Defense Finance and Accounting Service, Financial Systems Activity, Denver, Colorado, segregate the responsibilities for making program changes, performing system tests, and moving changed programs into production. This applies to the Defense Debt Management System and any other computer systems in which those responsibilities are currently performed by the same individual or group.*

Management Response. In its response to the draft audit report, FSA Denver concurred and stated that DDMS controls were put in place to comply with the recommendation. Moves to production were controlled and completed by personnel outside of both the testing and programming branches. Each branch performed a separate function (programming, testing, or moving programs to production). FSA Denver stated in its response that action on this recommendation was completed in July 1993.

Finding B. Software Change Management

Audit Followup. The Assistant Inspector General for Analysis and Followup closed Recommendation E.2. of IG, DoD, Report No. 94-060 based on the DFAS response to the report. However, as a result of our fieldwork, that recommendation has been reopened pending adequate action.

Results of Followup on Recommendation E.2. The Director, FSA Denver, had issued several memorandums to FSA Denver division chiefs emphasizing the importance of separation of duties. Each division chief had certified that separation of duties existed in his or her area. However, we found that adequate separation of duties did not exist for all central design activity divisions at FSA Denver. Specifically, DDMS application programmers had full access to the production library. DDMS management agreed that application programmers should not be given access to the production library and planned to establish a separate production control group. Once those actions have been completed, we will consider actions taken to be fully responsive.

Requirements for Coordination of Defense Joint Military Pay System

IG, DoD, Report No. 94-060, Recommendation E.3., "General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization." *We recommend that the Director, Defense Finance and Accounting Service, Financial Systems Activity, Denver, Colorado, enforce the coordination requirements established by Joint Service Software Directorate Operating Instruction 205-3 for making program changes to the Joint Service System for Active Components [now called the Defense Joint Military Pay System, Active Component] and the Joint Service System for Reserve Components [now called the Defense Joint Military Pay System, Reserve Component].*

Management Response. In its response to the original draft report, FSA Denver concurred and stated that it would reemphasize to all development personnel the necessity for full compliance with the requirements of JSS/DOI 205-3. All personnel were to be briefed on the requirements for segregation of duties for programming, testing, and moving programs to production. They were also to be briefed on the reasons for the certifier and programmer to be two different employees. Directorate-level formal policy statements would be issued to convey policy to all levels. The estimated completion date was February 15, 1994.

Results of Followup on Recommendation E.3. During our audit, we reviewed the implementation of the recommendation and found that the JSS/DOI 205-3 had been replaced by the DFAS-DE/FJ Instruction 5200.1 on November 29, 1993. As a result of poor coordination of that instruction, FSA Denver personnel did not comply with local requirements for authorization and approval of changes made to application programs.

Finding B. Software Change Management

DJMS Active Component. Although the DJMS Active Component had implemented operating procedures sufficient to ensure adequate separation of duties, personnel did not always perform certifications according to those procedures. This occurred because management did not enforce the coordination of DFAS Instruction 5200.1. A review of the 904 certification move sheets completed by the DJMS Active Component from February through August 1994 revealed that 320 (35.4 percent) were not performed in compliance with DFAS-DE/FJ Instruction 5200.1. Table 3 provides a detailed analysis of the discrepancies.

**Table 3. DJMS Active Component's Noncompliance
With DFAS-DE/FJ Instruction 5200.1**

<u>Type of Noncompliance</u>	<u>Number of Instances</u>	<u>Percentage of Total</u>
Programmer signed as analyst	295	32.6
Analyst did not sign certification	17	1.9
Other problems *	<u>8</u>	<u>0.9</u>
Total	320	35.4

*Other problems included deviations from DFAS-DE/FJ 5200.1. In some cases, no programmer signature was next to the typed name, and the programmer and certifier or the certifier and system analyst were the same individual.

DJMS Reserve Component. A review of the 147 certification move sheets completed by the DJMS Reserve Component from February through August 1994 revealed that 2 out of 147 sheets were improperly approved. That problem also requires management attention.

Summary

As shown by Table 4, DFAS management is implementing corrective actions on all four recommendations on software change management. Management's response to this report should provide the status of actions taken to satisfy recommendations listed as "in progress."

Finding B. Software Change Management

**Table 4. Status of Original Recommendations
on Software Change Management**

<u>Report Number</u>	<u>Recommendation</u>	<u>Management Action</u>
94-065	C.2.a.	In progress
94-060	E.1.	In progress
	E.2.	In progress
	E.3.	In progress

Recommendations, Management Comments, and Audit Response

1. We recommend that Director, Defense Finance and Accounting Service Financial Systems Activity, Pensacola, Florida:

a. Establish and implement local configuration management procedures for reviewing and approving changes to the Multiple Virtual Storage operating system.

Management Comments. The Deputy Director for Information Management, DFAS concurred. In December 1994, FSA Pensacola published and implemented Executive Software Configuration Management Procedures, which are based on the draft Executive Software Configuration Management Plan developed by FSA Pensacola and referenced in this report. By agreement between DFAS and DISA, DISA is assuming responsibility for the system maintenance and associated configuration management currently performed by FSA Pensacola. DISA will assume this responsibility by March 31, 1995. DFAS considers this recommendation completed.

Audit Response. Actions taken by FSA Pensacola are fully responsive to the recommendation. Due to the transfer of the operating responsibilities to the DISA, we have closed this recommendation and plan no additional followup work.

b. Provide Computer Associates' Network Management software training to appropriate personnel.

Management Comments. The Deputy Director for Information Management, DFAS, concurred. FSA Pensacola had intended to use CA-NETMAN software to support configuration management of operating system environments. However, since migration of operating system maintenance responsibilities to DISA was scheduled to be completed by March 31, 1995, efforts to establish a fully functional CA-NETMAN capability have been suspended. DFAS believes this recommendation should be transferred to DISA.

Finding B. Software Change Management

Audit Response. Due to the transfer of the operating responsibilities to the DISA, and because we were told that the DISA does not intend to use the CA-NETMAN software for configuration management, we have closed this recommendation.

2. We recommend that Director, Defense Finance and Accounting Service, Denver Center:

a. Finalize procedures currently in draft form for change management for all Financial Systems Activity Denver central design activities.

Management Comments. The Deputy Director for Information Management, DFAS, concurred. DFAS FSA Denver has finalized the draft procedure for change management. DFAS-FSA/DE Instruction 5200.1, "Software Change Control," was published November 8, 1994. These procedures are being followed, and a copy was provided to the IG, DoD, for review. DFAS considers this recommendation closed.

Audit Response. We reviewed DFAS-FSA/DE Instruction 5200.1 and concluded that the instruction clearly requires appropriate approvals and ensures management control of software changes. Therefore, we have closed this recommendation and plan no additional followup work.

b. Establish a separate production group for the Defense Debt Management System Division and implement procedures for segregating duties for making program changes, performing system tests, and moving changed programs into production for the Defense Debt Management System Division.

Management Comments. The Deputy Director for Information Management, DFAS, concurred. FSA Denver has segregated duties for making program changes, performing system tests, and moving changed programs into production for the DDMS. DFAS considers this recommendation closed.

Audit Response. After a June 7, 1995, followup visit to the FSA Denver, made jointly with a representative of the Assistant Inspector General for Analysis and Followup, we concluded that adequate separation of duties now exists for program changes, performing system tests, and moving changed programs into production. Therefore, we have closed this recommendation and plan no additional followup work.

c. Enforce coordination requirements for procedures to manage software changes.

Management Comments. The Deputy Director for Information Management, DFAS, concurred. Senior management continues to stress the importance of proper change control throughout FSA Denver. The Director has made this a major issue in management meetings, "all hands" meetings, and memorandums. This attention will continue, and spot-checks of change control procedures and documentation are scheduled. DFAS considers this recommendation closed.

Finding B. Software Change Management

Audit Response. After a June 7, 1995, followup visit to the FSA Denver, made jointly with a representative of the Assistant Inspector General for Analysis and Followup, we concluded that all 353 change control documents processed during April and May 1995 had been properly authorized. Therefore, we have closed this recommendation and plan no additional followup work.

This page was left out of original document

Part III - Additional Information

Appendix A. Summary of Potential Benefits Resulting From Audit

Recommendation Reference	Description of Benefit	Type of Benefit
A.1.a.	Management controls. Require password length according to DoD criteria. Decrease the risk of unauthorized access.	Nonmonetary
A.1.b.	Management controls. Limit started task access to specific files. Decrease the risk of unauthorized access.	Nonmonetary
A.2.	Compliance. Ensure that adequate controls exist over access to sensitive data.	Nonmonetary
B.1.a., B.1.b.	Management controls. Improve controls over the operating system.	Nonmonetary
B.2.a., B.2.b., B.2.c.	Management controls. Ensure that adequate controls exist over changes made to application programs.	Nonmonetary

Appendix B. Organizations Visited or Contacted

Office of the Secretary of Defense

Assistant Secretary of Defense (Command, Control, Communications and Intelligence),
Washington, DC

Defense Agencies

Defense Finance and Accounting Service, Arlington, VA
Defense Finance and Accounting Service Denver Center, Denver, CO
Defense Finance and Accounting Service Financial Systems Activity,
Denver, CO
Defense Finance and Accounting Service Indianapolis Center, Indianapolis, IN
Defense Finance and Accounting Service, Financial Systems Activity,
Pensacola, FL
Defense Information Systems Agency Western Hemisphere, Arlington, VA
Defense Information Systems Agency, Fort Richie, MD
Defense Information Services Organization, Arlington, VA

Other Defense Organizations

Department of Defense Computer Security Center, Fort George G. Meade, MD

Non-Defense Federal Organizations

Federal Emergency Management Agency, Atlanta, GA
Federal Emergency Management Agency, Baltimore, MD
National Institute of Standards and Technology, Gaithersburg, MD

Non-Federal Government Organizations

Western Florida Regional Planning Council, Pensacola, FL

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
Deputy Under Secretary of Defense (Financial Management)
Director, Management Improvement, Office of the Deputy Under Secretary of
Defense (Financial Management)
Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
Assistant to the Secretary of Defense (Public Affairs)
Director, Defense Logistics Studies Information Exchange

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Defense Agencies

Director, Defense Information Systems Agency
Director, Defense Information Services Organization
Director, Defense Finance and Accounting Service
Director, Defense Finance and Accounting Service Denver Center
Director, Defense Finance and Accounting Service Indianapolis Center
Director, Defense Finance and Accounting Service, Financial Systems Activity
Pensacola
Director, Defense Information Processing Center Pensacola
Director, Defense Logistics Agency

Defense Agencies (cont'd)

Director, Defense Contract Audit Agency
Directory, National Security Agency
Inspector General, National Security Agency

Non-Defense Organizations

Office of Management and Budget
Technical Information Center, National Security and International Affairs Division,
General Accounting Office

Chairman and ranking minority member of each of the following congressional
committees and subcommittees:

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Subcommittee on Force Requirements and Personnel, Committee on Armed
Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on National Security, Committee on Appropriations
House Subcommittee on Military Forces and Personnel, Committee on Armed Services
House Committee on Government Reform and Oversight
House Subcommittee on National Security, International Affairs, and Criminal Justice,
Committee on Government Reform and Oversight
House Committee on National Security

This page was left out of original document

Part IV - Management Comments

Under Secretary of Defense (Comptroller) Comments



COMPTROLLER

OFFICE OF THE UNDER SECRETARY OF DEFENSE
1100 DEFENSE PENTAGON
WASHINGTON, DC 20301-1100



APR 20 1995

MEMORANDUM FOR DIRECTOR, FINANCIAL MANAGEMENT DIRECTORATE
(ODOD IG)

SUBJECT: Audit of Corrective Action on System and Software
Security Deficiencies (Project No. 4FG-5060)

We appreciate the opportunity to review the draft of the
subject report. At this point, we have no objections to the
report findings and recommendations.

A handwritten signature in cursive script, appearing to read "Alvin Tucker".

Alvin Tucker
Deputy Chief Financial Officer

Defense Finance and Accounting Service Comments



DEFENSE FINANCE AND ACCOUNTING SERVICE

1931 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22240-5291

MAR 24 1995


DFAS-HQ/S

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL,
ATTN: Mr. C. Hendricks

SUBJECT: Audit of Corrective Action on System and Software
Security Deficiencies (Project No. 4FG-5060)

This responds to your memorandum of February 10, 1995, subject above. We appreciate the opportunity to provide comments on the follow on report. Specific Defense Finance and Accounting Service (DFAS) comments and suggested modifications to finding status are attached.

My point of contact for this action is Mr. Bob Graham, DFAS-HQ/SC, (703) 607-3963.


Robert E. Burke
Deputy Director for
Information Management

Attachment: As stated

Defense Finance and Accounting Service Comments

RECOMMENDATION COMMENTS/CORRECTIONS

- The Executive Summary should clearly explain that the follow on report was performed in August and that DoDIG findings and corrective actions after October 31, 1994, are NOT included. Any DoDIG references to findings or new DoD guidance after October 31, 1994, should be eliminated from the report and/or DFAS comments added with a note that the DODIG has not had time to validate these comments.
- The Executive Summary should state that the audit looked for weaknesses in internal controls and monetary impact. While several internal control weaknesses were found, there was no monetary loss or impact whatsoever revealed in any aspect of the audit.
- Page 2, correction, last para, line 5, "The Financial Services Organization", should read The Financial Systems Organization.
- Page 3, correction, first para, line 7 and 8, should read the Defense Joint Military Pay System, Active and Reserve Components. On the same page and para, line 9, "The Financial Services Organization", should read The Financial Systems Organization.
- Page 12 contains a finding on password length. It discusses eight character and five character passwords. New DISA guidance on passwords was not issued until December 1994, and DFAS did not receive the guidance until January 1995. DFAS did not want to shift from its five character password until DoD adopted a standard. The DoD/DISA guidance says that a minimum password of six characters will be used. This password length was adopted in the Defense Civilian Payroll System operating environment, at which your finding was directed, and has been operational since February 1995. DFAS considers this finding closed.
- Page 13 contains a finding on started tasks. It appears that your office has closed the issue regarding a draft Executive Software Configuration Management Plan. This document has been finalized and reissued as Executive Software Configuration Management Procedures. In response to this finding, started tasks were identified and tested in December 1994. Meanwhile, the "non-cancel" parameter which prevented jobs from aborting during transition testing was removed in January 1995, and any jobs not meeting the proper criteria are now automatically terminated. The executive software support function will transfer to DISA effective March 31, 1995 (it was expected to transfer on December 31, however, DISA requested an extension which was provided). DFAS considers this finding closed.
- Page 17, Recommendation A.1.a. Implement the use of passwords that have at least six characters. DFAS Response: Concur. Effective February 12, 1995, the password length requirement for the two platforms supported by FSAPE was modified to reflect a

Defense Finance and Accounting Service Comments

minimum of six characters. DFAS considers this recommendation closed.

- Page 17, Recommendation A.1.b. Complete testing and remove the "non-cancel" parameters from the started task jobs. DFAS Response: Concur. Effective January 1995, non-cancel was removed from all started tasks on the platforms supported by FSAPE thereby fully complying with the recommendation for this finding.

- Page 19, FSA Pensacola Operating System Change Management Procedures. As previously stated, FSAPE has finalized and reissued their Configuration Management Plan as a Configuration Management Procedure. As your report indicated, the use of an automated support tool CA-NETMAN is a fairly large project and contract support was to be used to obtain the necessary expertise. However, with the transfer of executive software support to DISA effective March 31, 1995, work on implementing CA-NETMAN has been suspended. DISA may or may not chose to implement software management using this same methodology. DFAS considers its responsibility for this finding completed. Any follow on requirements should be transferred to DISA.

- Page 26, Recommendation B.1.a. Establish and implement local configuration management procedures for reviewing and approving changes to the Multiple Virtual Storage operating system. Response: Concur. In December 1994, FSAPE published and implemented Executive Software Configuration Management Procedures, which are based on the draft Executive Software Configuration Management Plan developed by FSAPE and referenced in this report. By agreement between DFAS and Defense Information Systems Agency (DISA), operating system maintenance responsibility (and the configuration management associated therewith) currently performed by FSAPE is being assumed by DISA. Assumption of this responsibility will take place by March 31, 1995. DFAS considers this recommendation completed.

- Page 26, Recommendation B.1.b. Provide Computer Associates' Network Management software training to appropriate personnel. Response: Concur. It had been FSAPE's intent to use Computer Associates Network Management (CA-NETMAN) software as the automated tool supporting configuration management of operating system environments. However, given that migration of operating system maintenance responsibilities to DISA is scheduled to be completed by March 31, 1995, efforts at establishing a fully functional CA-NETMAN capability have been suspended. DFAS believes this recommendation should be transferred to DISA.

- Page 26, Recommendation B.2.a. Finalize procedures currently in draft form for change management for all FSA Denver central design activities. Response: Concur. DFAS Financial Systems Activity (FSA) Denver has finalized the draft procedure for change management. DFAS-FSADE Instruction 5200.1, Software Change Control, was published November 8, 1994. These procedures

Defense Finance and Accounting Service Comments

were disseminated and mandated the same date and are being followed. In addition, a copy was previously provided the IG for review. DFAS considers this recommendation closed.

- Page 26, Recommendation B.2.b. Establish a separate production group for the Defense Debt Management System Division and implement procedures for segregating duties for making program changes, performing system tests, and moving changed programs into production for the Defense Debt Management System Division. Response: Concur. FSA Denver has segregated duties for making program changes, performing system tests, and moving changed programs into production for the Defense Debt Management System. DFAS considers the intent of this recommendation met and closed.

- Page 26, Recommendation B.2.c. Enforce coordination requirements for procedures to manage software changes. Response: Concur. Senior management continues to stress the importance of proper change control throughout FSADE. The Director has made this a major issue in management meetings, "all hands" meetings and in memorandums. This level of attention will continue and spot checks of change control procedures and documentation are scheduled. DFAS considers this recommendation closed.

Defense Information Systems Agency Comments



DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURT HOUSE ROAD
ARLINGTON, VIRGINIA 22204-2190



IN REPLY
REFER TO:

Inspector General

20 APR 1995

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
ATTN: Financial Management Directorate

SUBJECT: Audit of Corrective Action on System and Software
Security Deficiencies (Project No. 4FG-5060)

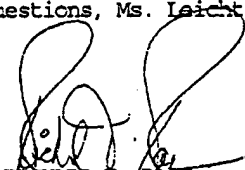
Reference: DoDIG Report, subject as above, 10 Feb 95

1. We reviewed the subject report per your request. The report found that keys to the computer backup tape storage facility at the Defense Information Processing Center (DIPC) Pensacola were not properly safeguarded. As a result, the operating system and payroll program could be subjected to unauthorized access.

2. We concur with the finding and the recommendation to implement safeguards over the keys to the storage facility. The DIPC Pensacola has taken the necessary steps to secure the keys to the tape backup facility. Those keys are locked in a key container within the equipment room of DIPC Pensacola. The DIPC Pensacola equipment room is a controlled area accessible to only those individuals who work in that area and have the appropriate background investigation. The key to the storage facility is controlled by the senior official on each shift. We believe this procedure is adequate protection for the tape backup storage area.

3. The point of contact for this action is Ms. Sandra Leicht, Audit Liaison. If you have questions, Ms. Leicht can be reached on (703) 607-6316.

FOR THE DIRECTOR:


RICHARD T. RACE
Inspector General

Quality Information for a Strong Defense

TOTAL P.02

Audit Team Members

Russell A. Rau
Christian Hendricks
Kent E. Shaw
Elaine M. Jennings
J. David Stockard
Melissa M. Fast
Susanne B. Allen
Traci Y. Sadler

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Corrective Actions on System and Software Security Deficiencies

B. DATE Report Downloaded From the Internet: 01/07/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date** 01/07/99

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.